Amendments to the Specification

Please replace the paragraph at page 12, lines 18-30, with the following amended paragraph:

The other main components of the host computer 100 attached to the PCI bus 225 include: a SCSI (small computer system interface) adaptor connected via a SCSI bus 235 to a hard disk drive ~~2600~~ 240 and a CD-ROM drive ~~2605~~ 245; a LAN (local area network) adaptor 250 for connecting the host computer 100 to a LAN 125, via which the host computer 100 can communicate with other host computers (not shown), such as file servers, print servers or email servers, and the Internet 130; an 10 (input/output) device 225, for attaching the keyboard 110, mouse 115 and smartcard reader 120; and a trusted device 260 (which incorporates the trusted display processor function). The trusted display processor handles all standard display functions plus a number of further tasks, which will be described in detail below. 'Standard display functions' are those functions that one would normally expect to find in any standard host computer 100, for example a PC operating under the Windows NTTM operating system, for displaying an image associated with the operating system or application software.

Please replace the paragraph at page 16, lines 26-31, with the following amended paragraph:

The measurement function 370 has access to: non-volatile memory 305,345 for storing a hash program 390 and a private key SDP of the trusted device 260, and volatile memory 335 for storing acquired integrity metric in the form of a digest ~~361~~. In appropriate embodiments, the volatile memory 335 may also be

used to store the public keys and associated ID labels ~~360a-360n~~ of one or more authentic smart cards 122 that can be used to gain access to the platform 100.

Please replace the paragraph at page 30, lines 10-33, with the following amended paragraph:

The user logs into a client trusted platform 1001, in preferred arrangement with the assistance of a user smart card 1008 connecting to the client trusted platform 1001 through a smart card reader 1007. The client trusted platform, smart card and interaction therebetween may be essentially as described in Figures 1 to 9 above (although this is not essential for implementation of all embodiments of the invention). Within the client trusted platform there is therefore a client trusted component 1003 which contains a display processor such that the output on the display 1005 is controlled by the client trusted component, and is therefore reliable. Also contained within the client trusted platform 1001 are an area of memory containing remote imaging code 1004 and an area of protected memory 1009. These need to be available for reliable use. Ideally, these might be sited within the trusted component 1003 itself-this however may result in the trusted component being expensive to produce (provision of some or all of the protected memory 1009 within a trusted component is a balance between security and cost). A potentially cheaper alternative, shown in Figure 10, is for the protected memory 1009 and the remote imaging code 1004 to be located outside the trusted component 1003 but connected to it by secure communication paths ~~1102~~ 1002 (preferably a dedicated communications link, ideally hardwired and isolated from any other components of the client trusted platform 1001,

essentially as described in Figures 8 and 9). If the protected memory 1009 and the remote imaging code 1004 are located on the client trusted platform in such a way that they are accessible to any component of the client trusted platform other than the client trusted component 1003, it is desirable at least that their integrity is monitored by the client trusted component, for example as described in the applicant's copending International Patent Application No. PCT/GB 00/02003 entitled